IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS

JONATHAN VILLAREAL, individually	**§**	
and derivatively on behalf of	**§**	
ZROBLACK, LLC.	**§**	
Plaintiffs,	**§**	
v.	**§**	**CIVIL ACTION NO. 5:20-cv-00571-OLG**
	§	
JOHN SAENZ, MIGUEL	**§**	
VILLARREAL, JR., and GUNN, LEE,	**§**	
& CAVE, P.C.	**§**	
Defendants	**§**	

UNSWORN DECLARATION OF JONATHAN VILLARREAL

1. My name is Jonathan Lee Villarreal. I am over eighteen years old; I am of sound mind and fully competent and capable of making this Declaration. I have never been convicted of a felony or other offense involving moral turpitude. The facts stated within this Declaration are within my personal knowledge and are true and correct.

2. I am the Owner of Zroblack, LLC. I currently have 3 patents pending on technologies based around security forensic data analysis. I have over 14 years of professional experience as a security engineer. My clients list as a professional security engineer includes Amazon, PayPal, AT&T, IBM, Procter & Gamble, Valero Energy, Verizon Wireless, GameStop, Starbucks, Adobe, Fox Corporation, Logitech, Glassdoor, Credit Karma, Hyatt Hotels, Uber, Yelp, Dropbox, and many more. I hold a Master of Science degree in Computer Science, with a specialty in security engineering. I was recognized and applauded for my Master's Thesis, "Detecting & Locating Improvised Explosive Devices With Mobile Device Based Detonators." I am currently a doctoral candidate in Computer Science, working on my thesis, "The Weaponization of Data Clearing, An Introduction to Connected Behavioral Forensics." I am

PLAINTIFF'S
EXHIBIT
45

known for my unique style of writing code, my hardware inventions, and my ability to perform forensic analysis, data clearing, and diagnostics rapidly and accurately on virtual and physical devices.

3. I have reviewed Steven Broderhausen's affidavit. Mr. Broderhausen is wrong when he states that "any proprietary code, data or other trade secrets capable of performing ZroBlack, LLC's ("ZroBlack") security services would be large in file size and plainly noticeable to Exhibit A in its forensic analysis." He is also wrong when he stated that no non-factory installed programming software was found on the computer. His affidavit demonstrates that he does not understand the nature of ZroBlack's code.

4. Exhibit 4 to Plaintiffs' Amended Application for Seizure or Alternatively Injunctive Relief (Doc. 37) identifies the intellectual property I assigned to ZroBlack. The assignment plainly states in the header "Solutions Available For: Windows OS, MacOS, OSX, Linux, Distros's, RaspbianOS" and "These solutions DO NOT install any apps, install any certificates, install mdm profiles, jailbreak, or modify the device in any way." Additionally, on page 4 it states, "These solutions DO NOT: Root the device, install 3rd party software, install any software at all."

5. I am the inventor and the author of every single line of code for which ZroBlack was paid. I have never needed to install programming software to help me write or execute code. This means my solutions do not require Integrated Development Environments (IDE), my solutions do not require launchers, helpers, cron jobs, or even an active internet connection. None of my software solutions have to be installed, nor can they be installed because that is not the type of proprietary code that I write. I do not have to install any applications that do not already come with a Mac, Windows, or Linux Operating system, which means, I do not need a specific version

of Python, Objective C, Ruby, Perl, or similar language. I do not have to install GOLang, package managers, a specific JAVA SDK, or any SDK; I do not have to install anything. My solutions do not install any applications. This means my solutions do not have any dependencies, I use all native tools which decrease the software size significantly.

6. Installation of dependencies or "programming software," in the industry is considered bloatware and old school. Installation of dependencies or "programming software" beyond natively found software causes security vulnerabilities that must be maintained, patched, versioned, supported, documented, and tested. Installation of dependencies or "programming software" slows down computer memory resources, CPU resources, and can cause conflicts with natively found programming software. Installation of dependencies or "programming software," can install drivers, libraries, text files, .ini files, .inf files, .exe, .dmg, .pkg, and more, that will prevent the type of code that I write from working.

7. Exhibit 39 attached to Plaintiffs' Amended Application for Seizure or Alternatively Injunctive Relief (Doc. 37) is the IP Due Diligence form provided to ZroBlack's Foreign Customer. Page 10 clearly states that there are no dependencies required to run these solutions. It lists an MIT license open-source reference document as "materials planned to be used." This is the only outside material used in my code.

8. The reason that Defendant Saenz's expert has not been able to find the proprietary code is because the numbers and letters that make up the code are saved in text files in the application Evernote, a cross-platform note taking application similar to Windows "Notepad" or its more robust open-source cousin "Notepad++." Applications such as Evernote, Notepad, and Notepad++ are commonly used by programmers to edit raw source code.

9. Exhibit 5 to Plaintiffs' Amended Application for Seizure or Alternatively Injunctive Relief (Doc. 37) is the receipt for the laptop in Saenz's possession and shows it was purchased on May 2, 2020. Evernote is installed on the laptop. I used "TeamViewer" to remotely access the computer and uploaded the text files containing ZroBlack's proprietary code to Evernote. TeamViewer is an application that allows one to remotely access a computer over the Internet. The code was stored in a private folder in an Evernote file format. There were six files: "ABD Device ID", "Clear MacOS iDevice Cached I/O", "Samsung ID – Commands, ADB Commands, Validation, Partial Diagnostics, Logging", "LG Device ID – Analytics, Logging", "Full Device ID & Diagnostics IOS", and "OSI Full Hardware Diagnostics." Because this code was stored in text files, the Saenz's expert likely did not see it or realize its significance.

10. The code contained in the files performs the following functions:

a. <u>ADB Device ID</u>

This code is used to access Android devices remotely.

b. <u>Clear MacOS iDevice Cached I/O</u>

This code allows access to iPhones and iPads from a Mac, or wirelessly, and clear the devices.

c. <u>Samsung ID - AT Commands, ADB Commands, Validation, Partial Diagnostics, Logging</u>

This code is used to perform forensics on Samsung Android devices.

d. <u>LG Device ID – Analytics, Logging</u>

This code is used to perform forensics on LG phones, tablets, and TVs running Android.

e. <u>Full Device ID and Diagnostics iOS</u>

This code is used to perform forensics on IOS devices, both through a wired connection to the device and wirelessly.

f. iOS Full Hardware Diagnostics

This code is used to perform forensics for hardware chipsets on IOS devices.

11. The Evernote text files are shown in Exhibit 42, which is the WorkChat log from Evernote showing these files are on the laptop.

12. To utilize the code, the user copies and pastes the code from the corresponding Evernote file to the Mac laptop's terminal command line. The Mac terminal command line is similar to the command prompt in Windows systems and command shell in Linux systems, which are text interfaces to the computer operating system. Once the user has copied and pasted the code to the Mac terminal command line, he executes it.

13. Furthermore, the hardware schematics are attachments to the iMessage application installed on the laptop's MacOS and are also attachments in Signal Messenger and Mac mail, both of which are present on the laptop.

14. On May 7th, 2019 in Tampere, Finland, I took a photo of John Saenz and the MacBook laptop computer he purchased. This is the laptop computer at issue in this lawsuit. A true and correct copy of that photo is attached as Exhibits 43 and 44. Exhibit 44 is a magnified version of the lower-left corner of Exhibit 43.

15. Exhibit 43 shows John wearing his passport pouch around his neck. The white power strip on the left only has slots for European plugs. The bottled water, Novelle, is sold in Finland Hartwell Ltd.

16. Exhibit 44 shows that John has a Mac terminal command line open while monitoring his stocks. The terminal icon appears in the lower left-hand corner of the photo. It is the leftmost icon on the Mac OS Dock. A "dot" appears under the icon, indicating it is open.

17. On May 9th, 2019, while in Tampere, Finland, I sent John code for him to test, so that it could be passed on to our foreign client's engineers. This code was sent to John through Evernote, and lives in a private container on the laptop. The files containing the code were named:

i. ADB Device ID
ii. Clear MacOS iDevice Cached I/O
iii. Samsung ID - AT Commands, ADB Commands, Validation, Partial Diagnostics, Logging…
iv. LG Device ID - Analytics, Logging
v. Full Device ID and Diagnostics iOS
vi. iOS Full Hardware Diagnostics

These are the same files discussed in paragraphs 11 and 12, above.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct. Executed on February 25, 2021.

____
Jonathan Lee Villarreal